UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

SANDRA VASQUEZ, individually, and on behalf of all others similarly situated, Plaintiff, v. NORTHWELL HEALTH, INC., and PERRY JOHNSON & ASSOCIATES, INC., Defendants.	Civil Action No.: 2:23-cv-8544 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff SANDRA VASQUEZ ("Plaintiff"), on behalf of herself and all others similarly situated, alleges the following Class Action Complaint against the above-captioned Defendants, Northwell Health, Inc. ("Northwell") and Perry Johnson & Associates, Inc. ("PJ&A") (collectively, the "Defendants"), upon personal knowledge as to herself and her own actions, and upon information and belief, including the investigation of counsel as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to safeguard her, and approximately 3.9 million other individuals' personally identifying information ("PII") and personal health information ("PHI"), including names, dates of birth, addresses, medical record numbers, encounter numbers, medical information, and dates/times of service.

2. Northwell is the largest healthcare system in New York and PJ&A is a third-party vendor of health information technology utilized by Northwell.

3. Between approximately March 27, 2023 and May 2, 2023, an unauthorized third party gained access to PJA's network system and obtained files containing information about Northwell's current and former patients (the "Data Breach" and/or "the Breach").

4. Defendants owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. Defendants breached that duty, by, among other things, failing to implement and maintain reasonable security procedures and practices to protect Northwell's patients' PII/PHI from unauthorized access and disclosure.

5. As a result of Defendants' inadequate security and breach of their duties and obligations, the Data breach occurred, and Plaintiff's and Class Members' PII/PHI was accessed and disclosed. Plaintiffs bring this action on behalf of herself and all persons whose PII/PHI was exposed as a result of the Breach, which occurred between approximately March 27, 2023, and May 2, 2023.

6. Plaintiff, on behalf of herself and all other Class members, asserts claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, unjust enrichment and violations of the New York Deceptive Acts and Practices Act, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

II. JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction pursuant to U.S.C. § 1332(d)(2) because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendants' citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

8. This Court has personal jurisdiction over Defendant Northwell because Northwell maintains its principal place of business in New Hyde Park, New York. Furthermore, Defendant Northwell intentionally and purposefully availed itself of this jurisdiction by marketing, employing individuals, and providing medical services in the state of New York.

9. This Court has personal jurisdiction over Defendant PJ&A because PJ&A intentionally and purposefully availed itself of this jurisdiction by choosing to do business in the state of New York.

10. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant Northwell is situated in this District, both Defendants conduct business in this District, and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District. Additionally, Plaintiff resides in this District.

III. PARTIES

Plaintiff SANDRA VASQUEZ

11. Plaintiff VASQUEZ is a resident and citizen of the State of New York, residing in Nassau County. Plaintiff was a patient at Northwell and, therefore, provided Northwell with her name, address, date of birth and PHI. Plaintiff received the Notice, dated November 3, 2023. By way of the Notice, Plaintiff was informed that her sensitive PII was compromised in the Data Breach.

Defendant Northwell

12. Defendant Northwell Health, Inc. is a New York not-for-profit corporation with its principal place of business located at 2000 Marcus Avenue, New Hyde Park, New York 11042.

Defendant PJ&A

13. Defendant Perry Johnson & Associates, Inc. is a Nevada corporation with its principal place of business located at 1489 W. Warm Springs Road, Henderson, Nevada 89014. It may be served through its registered agent C T Corporation System, 701 S. Carson Street, Suite 200, Carson City, Nevada 89701.

IV. FACTUAL ALLEGATIONS

Defendants' Businesses

14. Northwell is a major hospital system located in New York, providing care to citizens of New York as well as the surrounding states. Northwell has over 900 different locations where it provides service, with many of those locations clustered in or around Long Island, New York and New York City, New York.

15. PJA is a Nevada based corporation that, according to its website, "provides medical transcription services to various healthcare organizations." [1]

16. Northwell hired PJ&A, a medical technology company, for the transcription and dictation of Northwell's patient data, including the storage of Plaintiff's and Class members' PII. Like millions of New Yorkers, Plaintiff, and the Class members, provided its PII to Northwell for health purposes. In undertaking this responsibility, Northwell was obligated to only hire vendors who maintain adequate security measures.

[1] *See* https://www.pjats.com/.

17. In the ordinary course of working for or receiving health care services from Northwell, patients are required to provide, at a minimum, their PII. This PII is then paired with PHI attributable to a given patient, and the PHI then becomes identifiable as a result.

18. Prior to receiving care and treatment from Northwell, Plaintiff VASQUEZ was required to and did in fact turn over much of the private and confidential information listed in this Complaint.

19. Additionally, with respect to PHI, Northwell may receive private and personal information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, patients' other doctors, patient's health plan(s), close friends, and/or family members.

20. Northwell also creates and maintains a considerable amount of PHI while providing medical care and treatment. This PHI includes, but is not limited to, billing account numbers, financial information, medical record numbers, dates of service, provider names, and medical and clinical treatment information regarding care received from Northwell. All of this information is then provided to PJ&A for the purposes of transcription or dictation.

21. According to Northwell's website, "patients are our number one priority and we believe that patient privacy is an integral part of the health care we provide you."[2] The website continues, "[t]o ensure the development of a lasting bond of trust with our patients, we have many safeguards to protect the privacy and security of your personal information…We also have many policies in place to protect the privacy and security of your personal information and our employees are educated from the moment they are hired and continually after, to respect and protect patient privacy."[3]

[2] *See* https://www northwell.edu/about-northwell/commitment-to-excellence/protecting-patient-privacy
[3] *Id.*

22. According to Northwell's Notice of Privacy Practices (which can also be found on the Northwell website), "[we are] required by law to make sure that the information that identifies you is kept private."[4] And while the Notice of Privacy Practices discusses each of the various uses and disclosures of patient health information, it emphasizes that such uses and disclosures are only done so with written authorization. Thus, Northwell (and therefore, the third parties it hires, such as PJ&A) promises to maintain the confidentiality of patients' health, financial, and non-public personal information, ensure compliance with federal and state laws and regulations, and not to use or disclose patients' health information for any reasons other than those expressly listed in the Privacy Notice without written authorization.

23. Due to the highly sensitive and personal nature of the information Northwell acquires, Northwell recognizes patients' right to privacy on its website, and it promises in its Notice of Privacy Practices, to, among other things, maintain the privacy of patients' protected health information, which includes the types of data compromised in the Data Breach.

24. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class members' PII, Defendants assumed legal and equitable duties and knew that they were responsible for protecting Plaintiff's and Class members' PII from unauthorized disclosure.

25. Plaintiff and the Class members have taken reasonable steps to maintain the confidentiality of their PII.

[4] *See* https://www northwell.edu/sites/northwell.edu/files/d7/21620_Notice%20of%20privacy%20practices_booklet_FINAL.pdf

26. Plaintiff and the Class members relied on Defendants to keep their PII confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information.

The Data Breach

27. Between approximately March 27, 2023 and May 2, 2023, "an authorized party gained access to the PJ&A Network…and, during that time, acquired copies of certain files from PJ&A Systems."

28. According to the Notice of Data Security Incident posted on PJA's website, the PI/PHI affected in the Data Breach included names, dates of birth, addresses, medical record numbers, hospital account numbers, admission diagnoses, dates and times of service, Social Security numbers, insurance information, clinical information such as laboratory and diagnostic testing results, medications, treatment facility names, and healthcare provider names.[5]

29. Northwell's Notice of Privacy Practices states, "You have a right to be notified in the event of a breach of the privacy of your unsecured protected health information by Northwell Health or its business associates."[6] The Notice of Privacy Practices promises patients that they "will be notified as soon as reasonably possible, but no later than 60 days following our discovery of the breach." Northwell learned of the breach on or about July 21, 2023 but did not disclose the breach to its patients until early November, 2023, over three months later.[7]

30. Northwell's failure to promptly notify Plaintiff and class members that their PII/PHI was accessed and stolen virtually ensured that the unauthorized third parties who exploited those

[5] *See* https://pjats.com/downloads/Notice.pdf
[6] *See* https://www northwell.edu/sites/northwell.edu/files/d7/21620_Notice%20of%20privacy%20practices_booklet_FINAL.pdf
[7] *See* https://www hipaajournal.com/northwell-health-pja-data-breach/.

security lapses could monetize, misuse, or disseminate that PHI/PII before Plaintiff and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and Class members will suffer indefinitely from the substantial and concrete risk that their identifies will be (or already have been) stolen and misappropriated.

Defendants Knew that Criminals Target PI/PHI

31. At all relevant times, Defendants knew, or should have known, that the information they collected was a target for malicious actors. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class Members' PII/PHI from cyber-attacks that Defendants should have anticipated or guarded against.

32. It is well known amongst companies that store sensitive personally identifying information that information, such as the PHI/PII stolen in the Data Breach, is valuable and frequently targeted by criminals.

33. Simply put, PHI/PII is valuable to hackers. For example, "healthcare records are so valuable because they can be used to commit a multitude of crimes."[8] Specifically, "Healthcare data can be used to impersonate patients to obtain expensive medical services, Medicare and Medicaid benefits, healthcare devices, and prescription medications. Healthcare records also contain the necessary information to allow fraudulent tax returns to be filed to obtain rebates."[9]

34. Stolen PHI/PII can be "processed and packaged with other illegally obtained data to create full record sets that contain extensive information on individuals, often in intimate detail.

[8] *See* https://www hipaajournal.com/why-do-criminals-target-medical-records
[9] *Id.*

These full record sets are often sold on dark web sites to other criminals who use the data to obtain documentation such as Social Security cards, driver's license numbers, and passports."[10]

35. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII/PHI Has Serious and Long-Lasting Consequences for Victims

36. The theft of PHI/PII has serious and long-lasting consequences for victims, such as Plaintiff and class members here. One such lasting consequence is identity theft. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). Further, identifying information is "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person." 12 C.F.R. § 1022.3(g)

37. Identity theft is a complex issue that is not easily remedied. In a survey, the Identity Theft Resource Center found that almost 20% of victims of identity misuse needed more than a month to resolve issues stemming from identity theft.[11] Theft of PII is even more egregious when it includes theft of PHI. Data breaches involving medical information leave "a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[12] Alarmingly, the FTC warns that "[i]f the thief's health information is mixed with yours it could affect the medical care, you're able to get or the health insurance benefits you're able to use."[13]

---

[10] *Id.*
[11] *See* https://www.idtheftcenter.org/publication/2023-consumer-impact-report/.
[12] *See* https://www.worldprivacyforum.org/wp.content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf
[13] *See* https://consumer ftc.gov/articles/what-know-about-medical-identity-theft

38. Theft of Social Security Numbers ("SSN") also creates a particularly alarming situation for victims because SSNs cannot easily be replaced. To obtain a new SSN, a breach victim must demonstrate ongoing harm from misuse of her SSN. Thus, a new SSN will not be provided until after the harm has already been suffered by the victim. A stolen SSN, in combination with other PII (e.g., name, address, date of birth) presents an even more precarious situation to the victim.

Damages Suffered by Plaintiff and Class Members

39. Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for services that were received without adequate data security.

CLASS ALLEGATIONS

40. Plaintiff brings this class on behalf of herself and all other similarly situated class members ("the Classes") pursuant to Rule 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure and seeks certification of the following Class against Defendants for violations of New York state laws and/or similar laws in other states:

Nationwide Class Action

All United States residents whose PI/PHI was accessed by and disclosed to unauthorized persons in the Data Breach, including all that were sent a notice of the Data Breach.

41. Excluded from proposed classes are the Defendants, any entity or entities in which Defendants have a controlling interest, Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns.

42. Also excluded from the Nationwide Class any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

43. The members of the Class are so numerous that joinder of all members of the Class is impracticable. Plaintiff is informed and believes that the proposed Class contains millions of victims of the Data Breach who have been damaged by Defendants' conduct as alleged herein. The precise number of class members is unknown to Plaintiff currently.

44. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

45. Plaintiff's claims are typical to those of all Class members because members of the Class are similarly injured through Defendants' uniform misconduct described above and were subject to Defendants' conduct as alleged herein. Plaintiff is advancing the same claims and legal theories on behalf of herself and all members of the Class.

46. Plaintiff's claims raise questions of law and fact common to all members of the Class, and they predominate over any questions affecting only individual class members. These common legal and factual questions include, but are not limited to:

a. Whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class members' PII/PHI from unauthorized access and disclosure;

b. Whether Defendants had duties not to disclose the PII/PHI of Plaintiff and Class members to unauthorized third parties;

c. Whether Defendants failed to exercise reasonable care to secure and safeguard Plaintif's and Class members PII/PHI;

d. Whether an implied contract existed between Class members and Defendants, providing that Defendants would implement and maintain reasonable security measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;

e. Whether Defendants breached their duties to protect Plaintiff's and Class Members PII/PHI; and

f. Whether Defendants and Class Members are entitled to damages and the measures of such damages and relief.

47. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

48. Plaintiff will fairly and adequately represent and adequately protect the interests of the Class members in that she has no disabling or disqualifying conflicts of interest that would be antagonistic to those of the other members of the Class. The damages and infringement of rights Plaintiff suffered are typical of other Class members, and Plaintiff seeks no relief that is

antagonistic or adverse to the members of the Class. Plaintiff has retained counsel experienced in complex class action litigation, including data breach class action litigation, and Plaintiff intends to prosecute this action vigorously.

49. Furthermore, a class action is superior to other available methods for the adjudication of this litigation since individual litigation of the claims of Plaintiff and the members of the proposed Class is impracticable. It would be unduly burdensome to the courts in which the many thousands of individual actions would proceed. Also, individual litigations would present a potential for inconsistent or contradictory judgments, and inevitably increase the delay and expense to all parties and the courts in resolving the legal and factual issues of these cases.

COUNT I

NEGLIGENCE

50. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

51. Defendants owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting the PII/PHI in their possession, custody, or control.

52. Defendants knew or should have known the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining secure systems. Defendants knew or should have known of the many data breaches that targeted healthcare providers in recent years.

53. Given the nature of Defendants businesses, the sensitivity and value of the PII/PHI they maintain, and the resources at their disposal, Defendants should have identified the vulnerabilities to their systems or their third-party vendor's systems and prevented the Data Breach from occurring.

54. Defendants breached these duties by failing to, or contracting with companies that failed to, exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to, or contracting with companies that failed to, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it, including Plaintiff's and Class members' PII/PHI.

55. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to, or contracting with companies that failed to, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

56. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised.

57. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remain in Defendants' possession; (vi) future costs in terms of time, effort and money that will be required to prevent, detect and repair the impact of the PII/PHI compromised as a result of the

Data Berach; and (vii) overpayment for the services that were received without adequate data security.

COUNT II

NEGLIGENCE PER SE

58. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

59. Defendants' duties arise from, inter alia, the HIPAA Privacy Rule ("standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. § Part 160 and § Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. § Part 160 and § Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

60. Defendants' duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. §45 (a) (1), which prohibits "unfair…practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as Northwell, of failing to employ reasonable measures to protect and secure PII/PHI.

61. Defendants violated HIPAA Privacy and Security Rules, Section 5 of the FTCA, and IPIPA by failing to, or contracting with companies that failed to, use reasonable measures to protect Plaintiff's and other Class members' PII/PHI, by failing to provide timely notice, and by not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII/PHI they obtain and store, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

62. Defendants' violation of the HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence *per se*.

63. Plaintiff and Class members are within the class of persons that the HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

64. The harm occurring as a result of the Data Breach is the type of harm that the HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiff and Class members as a result of the Data Breach.

65. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to, or contracting with companies that failed to, design, adopt, implement, control, direct, oversee, manage monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

66. The injury and harm that Plaintiff and other Class members suffered was the direct and proximate result of Defendants' violations of harm, the HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (a) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent,

detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT III

BREACH OF FIDICUARY DUTY

Against Northwell Only

67. Plaintiff realleges and incorporates by reference all preceding paragraphs as is fully set forth herein.

68. This is claim is brought by Plaintiff on behalf of all Class members who provided their PII/PHI to Northwell.

69. Plaintiff and class members gave Northwell their PII/PHI in confidence, believing that Northwell would protect that information. Plaintiff and Class members would not have provided Northwell with this information had they known it would not be adequately protected. Northwell's acceptance and storage of Plaintiff's and Class Members' PII/PHI created a fiduciary relationship between Northwell and Plaintiff and Class members. Considering this relationship, Northwell must act primarily for the benefit of its patients, which includes safeguarding and protecting Plaintiff's and Class Members' PII/PHI.

70. Due to the nature of the relationship between Northwell and Plaintiff and Class members, Plaintiff and Class members were entirely reliant upon Northwell to ensure that their PII/PHI was adequately protected. Plaintiff and Class members had no way of verifying or influencing the nature and extent of Northwell's or its vendors data security policies and practices, and Northwell was in an exclusive position to guard against the Data Breach.

71. Northwell has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. They breached that duty by contracting with companies that failed to properly protect the integrity of the system containing Plaintiff's and Class

Members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class members' PII/PHI that they collected.

72. As a direct and proximate result of Northwell's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (a) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security

COUNT IV

BREACH OF IMPLIED CONTRACT

Against Northwell Only

73. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

74. This claim is brought by Plaintiff on behalf of all Class members who provided their PII/PHI to Northwell.

75. In connection with receiving healthcare services, Plaintiff and all other Class members entered implied contracts with Northwell. Pursuant to these implied contracts, Plaintiff and Class members paid money to Northwell, directly or through their insurance, and provided Northwell with their PII/PHI. In exchange, Northwell agreed to, among other things, and Plaintiff and Class members understood that Northwell would: (1) provide services to Plaintiff and Class

members; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI; and (3) protect Plaintiff's and Class members' PII/PHI in compliance with federal and state laws and regulations and industry standards.

76. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Northwell, on the other hand. Indeed, as set forth supra, Northwell recognized the importance of data security and the privacy of Northwell's patients' PII/PHI. Had Plaintiff and Class members known that Northwell would not adequately protect their PII/PHI, they would not have received healthcare or other services from Northwell.

77. Plaintiff and Class members performed their obligations under the implied contract when they provided Northwell with their PII/PHI and paid for healthcare or other services from Northwell.

78. Northwell breached its obligations under its implied contracts with Plaintiff and secure their PII/PHI, including by ensuring companies it contracts with implement and maintain reasonable security measures to protect PII/PHI, and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

79. Northwell's breach of its obligations of its implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class members have suffered from the Data Breach.

80. Plaintiff and all other Class members were damaged by Northwell's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they

are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) overpayment for services that were received without adequate data security.

COUNT V

UNJUST ENRICHMENT

81. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

82. This claim is pleaded in the alternative to the breach of implied contract claim.

83. Plaintiff and Class members conferred a monetary benefit upon Defendants in the form of monies paid to Northwell for healthcare services, which Northwell used in turn to pay for PJA's services, and through the provision of their PII/PHI.

84. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiff and Class members. Defendants also benefitted from the receipt of Plaintiff's and Class members' PII/PHI, as this was used to facilitate billing services and services provided to Northwell.

85. As a result of Defendants' conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

86. Defendants should not be permitted to retain the money belonging to Plaintiff and Class members because Defendants failed to adequately implement the data privacy and security procedures for themselves that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

87. Plaintiff and Class members have no adequate remedy at law.

88. Defendants should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by them as a result of the conduct and Data Breach alleged herein.

COUNT VI

VIOLATIONS OF THE NEW YORK DECEPTIVE ACTS AND PRACTICES ACT, N.Y. Gen. Bus. Law § 349 ("GBL")

Against Northwell Only

89. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

90. New York General Business Law § 349(a) states, "Deceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful."

91. Northwell is a "person, firm, corporation or association or agent or employee thereof" within the meaning of the GBL. N.Y. Gen. Bus. Law § 349(b). At all relevant times, Northwell was engaged in "business," "trade," or "commerce" within the meaning of the GBL. See N.Y. Gen. Bus. Law § 349(a).

92. Plaintiff and Class members are "persons" within the meaning of Gen. Bus. Law § 349(h).

93. Northwell promised to protect, but subsequently failed to adequately safeguard and maintain, Plaintiff's and Class members' PII/PHI. Northwell failed to notify Plaintiff and other Class members that, contrary to its representations about valuing data security and privacy, it does not maintain adequate controls to protect their PII/PHI, including by ensuring companies it contracts with maintain adequate data protection practices.

94. Had Plaintiff and Class members been aware that Northwell omitted or misrepresented facts regarding the adequacy of its data security safeguards, Plaintiff and Class members would not have accepted services from Northwell.

95. Northwell's failure to make Plaintiff and Class members aware that it would not adequately safeguard their information, while maintaining that it would, is a "deceptive act or practice" under N.Y. Gen. Bus. Law § 349.

96. Plaintiff and all other Class members were damaged by Northwell's unfair and deceptive trade practices because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) overpayment for services that were received without adequate data security.

97. Pursuant to Gen. Bus. Law § 349(h), Plaintiff seeks damages on behalf of himself and Class members in the amount of the greater of actual damages or $50 for each violation of

N.Y. Gen. Bus. Law § 349. Because Northwell's conduct was committed willfully and knowingly, Plaintiff and Class members are entitled to recover up to three times their actual damages, up to $1,000.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on her own behalf and on behalf of all others similarly situated, prays for relief as follows:

A. For an Order certifying this case as a class action and appointing Plaintiff and her counsel to represent the Class;

B. For an award of actual damages, compensatory damages, statutory damages, nominal damages and statutory penalties, in an amount to be determined, as allowable by law;

C. For an award of punitive damages, as allowable by law;

D. For injunctive and other equitable relief to ensure the protection of the sensitive information of Plaintiff and the Class which remains in Defendants' possession;

E. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

F. Pre- and post-judgment interest on any amounts awarded; and

G. Such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff respectfully request a trial by jury on all causes of action so triable.

Dated: November 16, 2023

Respectfully Submitted,

PARKER WAICHMAN LLP

/s/ Raymond C. Silverman

Raymond C. Silverman
Jason S. Goldstein
6 Harbor Park Drive
Port Washington, NY 11050
Phone: (516) 466-6500
Fax: (516) 466-6665
rsilverman@yourlawyer.com
jgoldstein@yourlawyer.com